Comprehensive Cross-Domain Enterprise Threat Exposure Analysis

Greg Conti
Bob Fanelli

The views expressed in this talk are those of the authors and do not reflect the official policy or position of Kopidion, the United States Government, or any of our other current or past employers.

Greg Conti
Principal, Kopidion
@cyberbgone

Bob Fanelli
Principal, Kopidion

KOPIDION™

He’s intelligent,
but not experienced.
His pattern indicates
two dimensional
thinking.

He followed me
this far. He’ll be
back. But from
where?

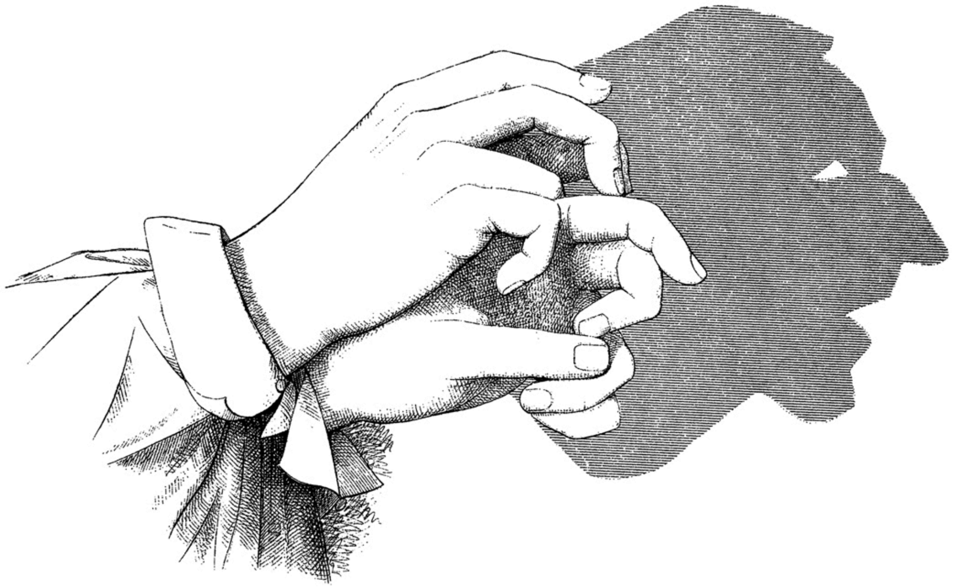
https://www.youtube.com/watch?v=iPQfwmfRq2s

Z-10,000 meters…
Standby photo torpedoes

USS ENTERPRISE
NCC-1701

FIRE!

Problem



Imagine your organization’s projection into cyberspace and physical space.

- **Defenders** fail to consider the entire projection of their organization in virtual and physical space.
- **Attackers** understand this and find un(der)-protected areas, often at gaps and seams to exploit.

Is it possible to create a framework that enables repeatable holistic analysis?

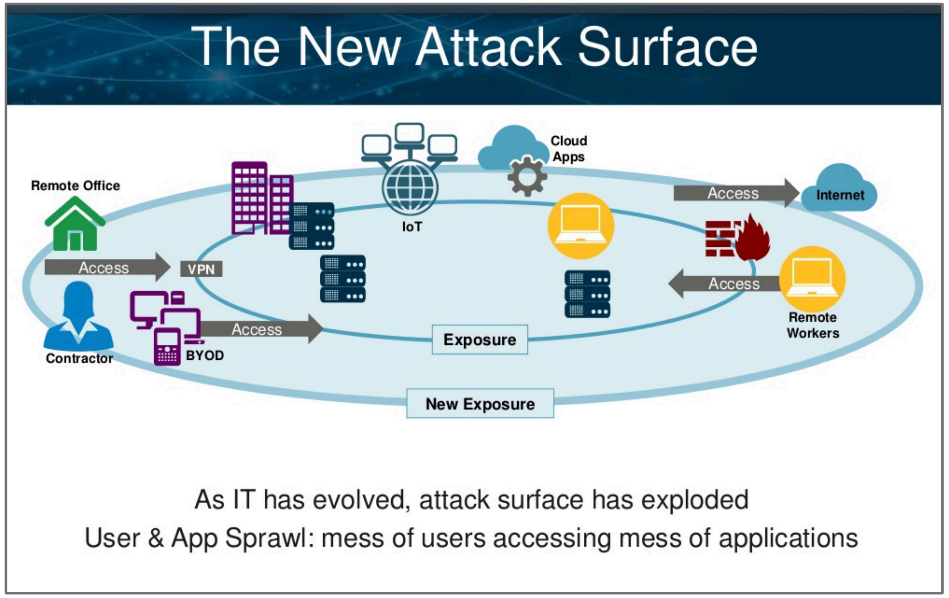
https://thegraphicsfairy.com/unusual-shadow-puppet-printable/

Why, So What, Who Cares?

- There are literally armies operating in cyberspace.
- Current attack surface analysis is a good start, but insufficient.
- All enterprise defenders (including red teamers) can benefit from a framework that supports comprehensive multi-domain analysis
- Analysis assists in prioritized allocation of scarce security resources.

https://hearinghealthmatters.org/wp-content/uploads/sites/16/files/2020/08/whisper.jpg

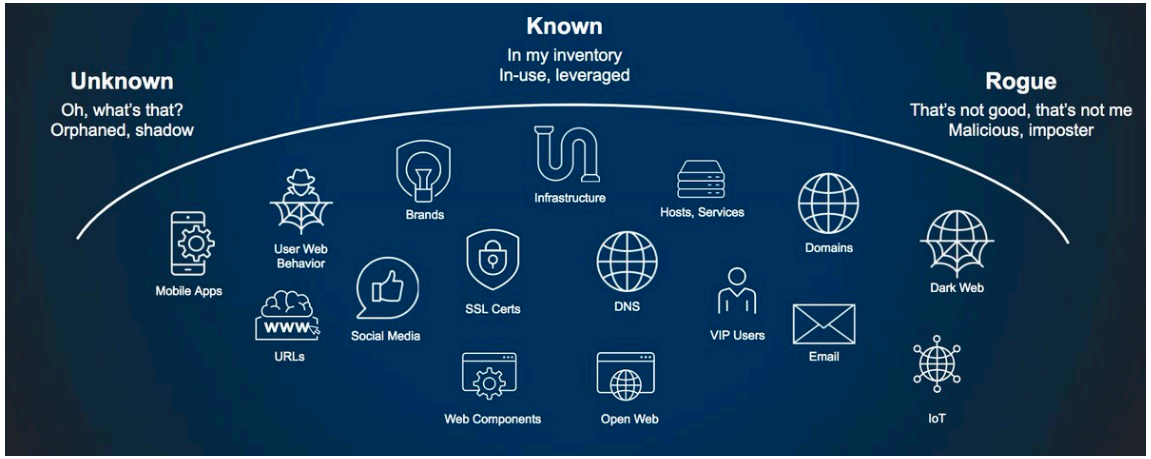
Related Work

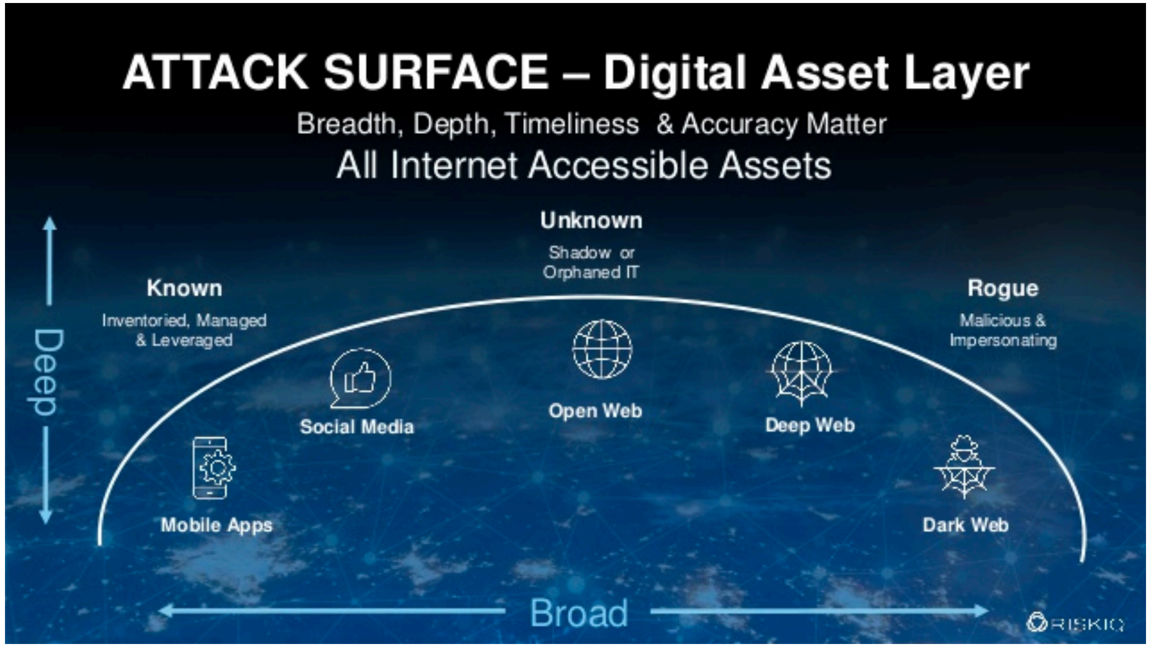


The New Attack Surface

As IT has evolved, attack surface has exploded
User & App Sprawl: mess of users accessing mess of applications

Intellyx/Certes Networks, "The Cyber House of Horrors: Securing the Expanding Enterprise Attack Surface," Webinar, 2016 Slides



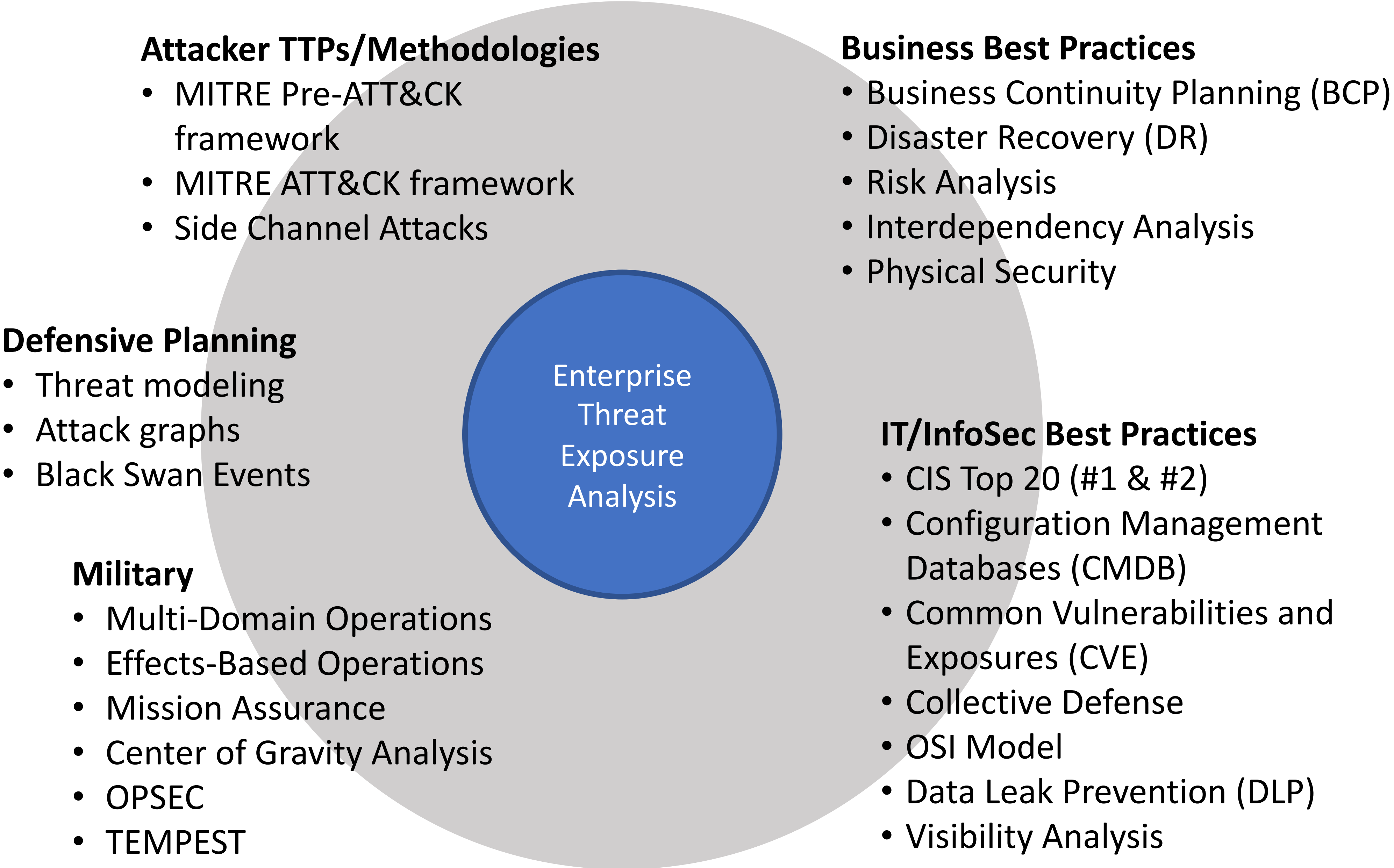


ATTACK SURFACE – Digital Asset Layer

Breadth, Depth, Timeliness & Accuracy Matter
All Internet Accessible Assets

RiskIQ, "Analysis of an Attack Surface," White Paper, 2020 Link

Linkages



Enterprise Threat Exposure Analysis

Attacker TTPs/Methodologies
- MITRE Pre-ATT&CK framework
- MITRE ATT&CK framework
- Side Channel Attacks

Business Best Practices
- Business Continuity Planning (BCP)
- Disaster Recovery (DR)
- Risk Analysis
- Interdependency Analysis
- Physical Security

Defensive Planning
- Threat modeling
- Attack graphs
- Black Swan Events

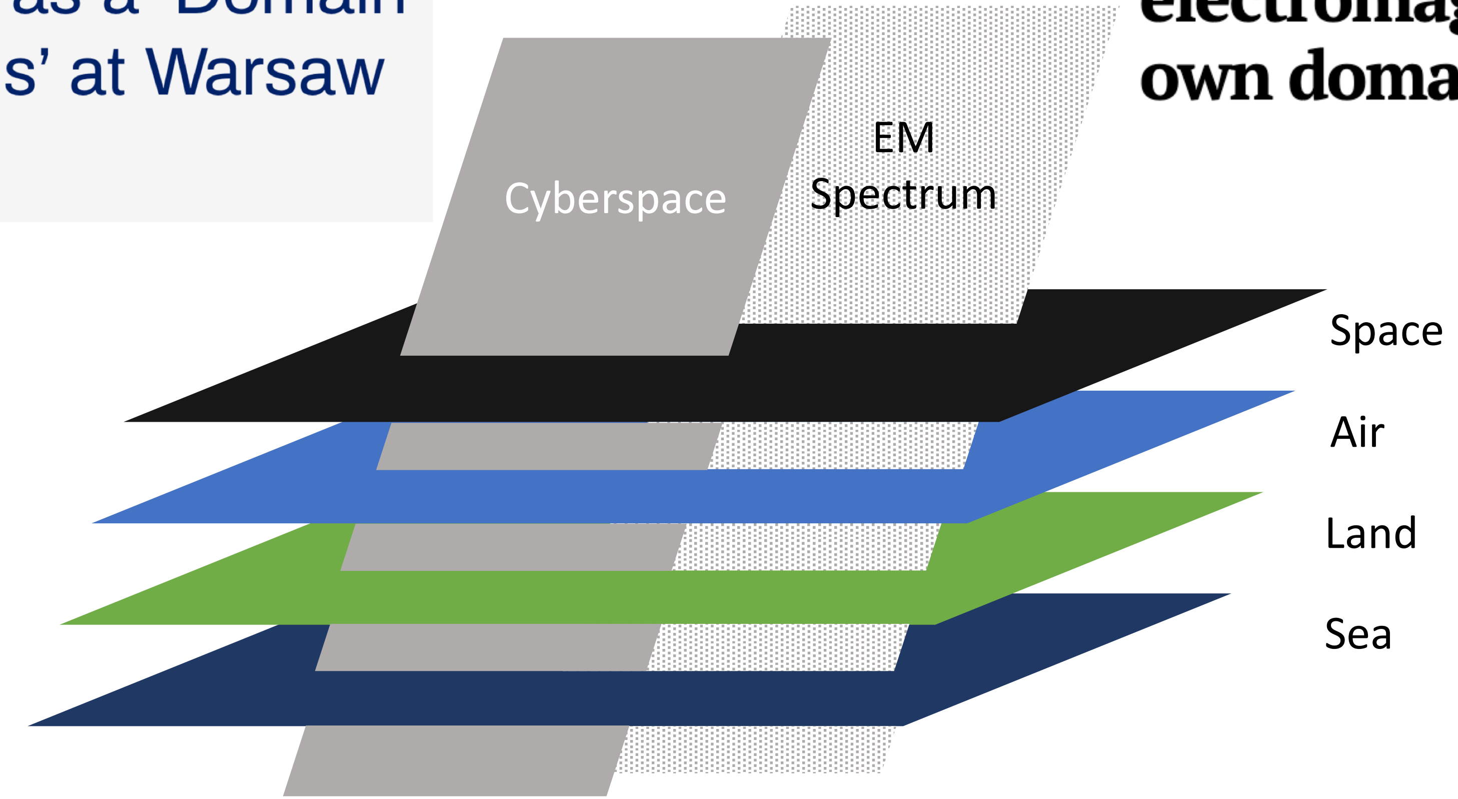
IT/InfoSec Best Practices
- CIS Top 20 (#1 & #2)
- Configuration Management Databases (CMDB)
- Common Vulnerabilities and Exposures (CVE)
- Collective Defense
- OSI Model
- Data Leak Prevention (DLP)
- Visibility Analysis

Military
- Multi-Domain Operations
- Effects-Based Operations
- Mission Assurance
- Center of Gravity Analysis
- OPSEC
- TEMPEST

Operational Domains

CCDCOE

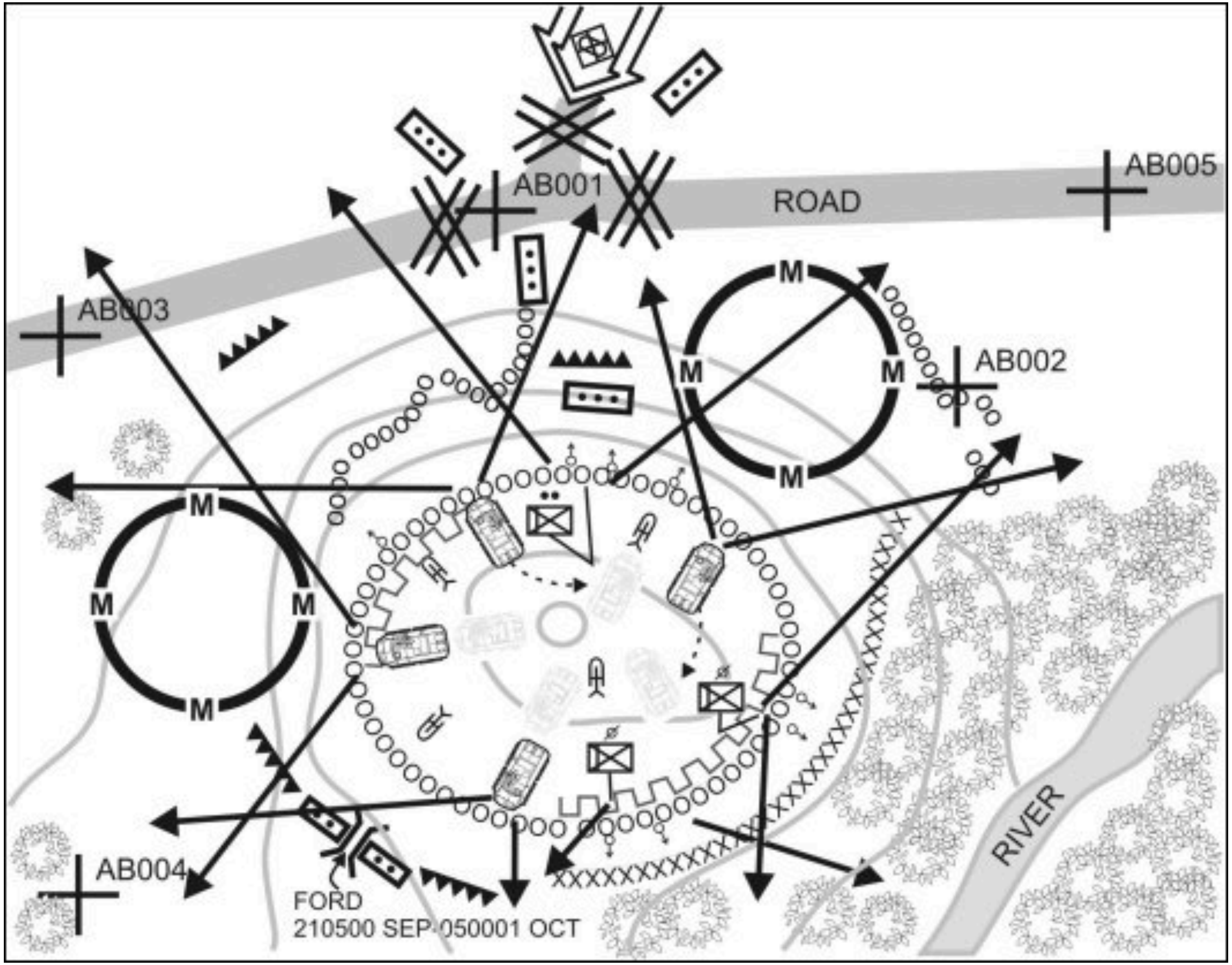
NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit

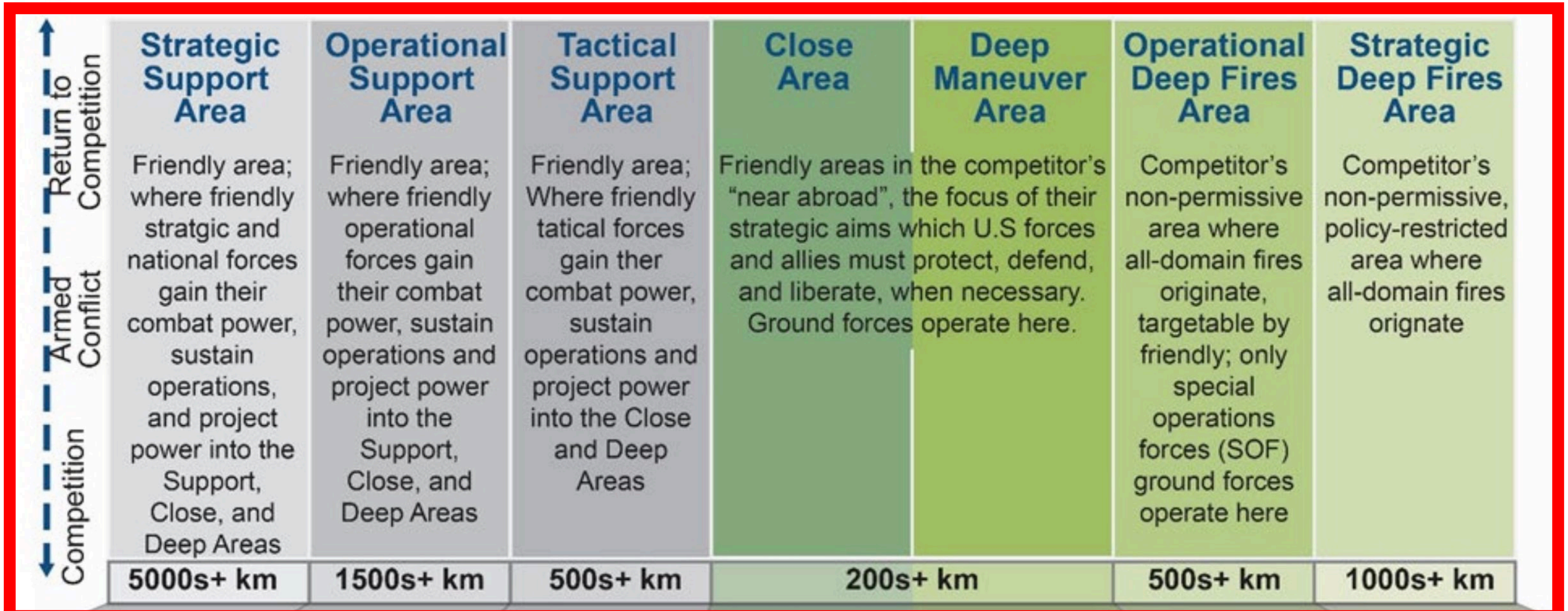


DefenseNews

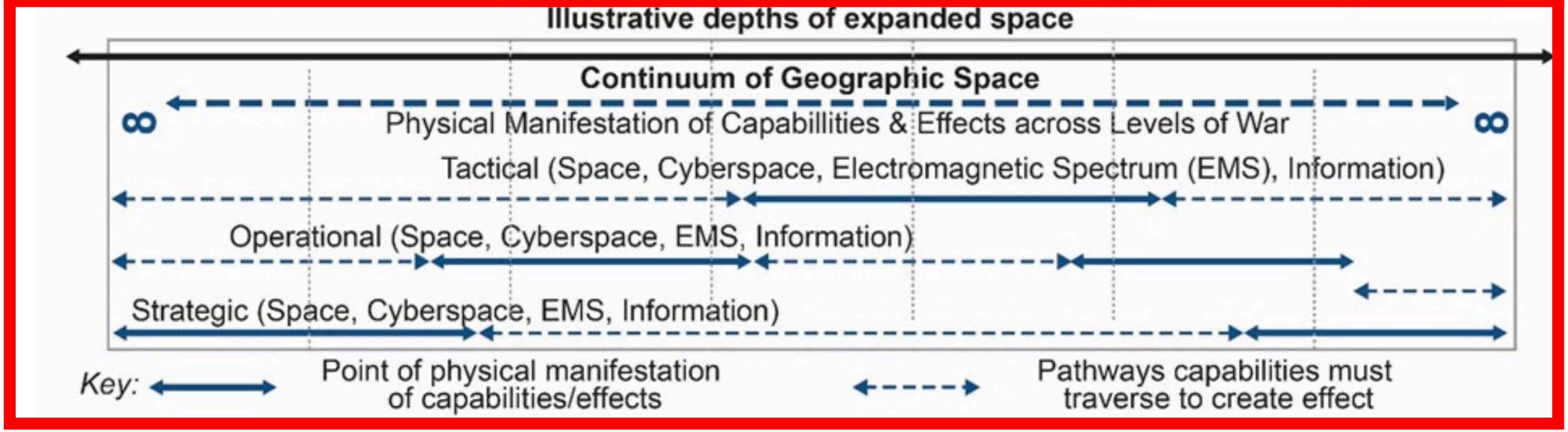
Should the military treat the electromagnetic spectrum as its own domain?

https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/
https://www.defensenews.com/electronic-warfare/2019/11/06/should-the-military-treat-the-electromagnetic-spectrum-as-its-own-domain/


AB005
ROAD
AB001
AB003
M
M
M
M
AB002
M
M
M
M
RIVER
AB004
FORD
210500 SEP-050001 OCT


Return to Competition
Armed Conflict
Competition

Strategic Support Area	Operational Support Area	Tactical Support Area	Close Area	Deep Maneuver Area	Operational Deep Fires Area	Strategic Deep Fires Area
Friendly area; where friendly stratgic and national forces gain their combat power, sustain operations, and project power into the Support, Close, and Deep Areas	Friendly area; where friendly operational forces gain their combat power, sustain operations and project power into the Support, Close, and Deep Areas	Friendly area; Where friendly tatical forces gain ther combat power, sustain operations and project power into the Close and Deep Areas	Friendly areas in the competitor's "near abroad", the focus of their strategic aims which U.S forces and allies must protect, defend, and liberate, when necessary. Ground forces operate here.		Competitor's non-permissive area where all-domain fires originate, targetable by friendly; only special operations forces (SOF) ground forces operate here	Competitor's non-permissive, policy-restricted area where all-domain fires orignate
5000s+ km	1500s+ km	500s+ km	200s+ km		500s+ km	1000s+ km



Illustrative depths of expanded space

Continuum of Geographic Space

∞ Physical Manifestation of Capabillities & Effects across Levels of War ∞

Tactical (Space, Cyberspace, Electromagnetic Spectrum (EMS), Information)

Operational (Space, Cyberspace, EMS, Information)

Strategic (Space, Cyberspace, EMS, Information)

Key: Point of physical manifestation of capabilities/effects; Pathways capabilities must traverse to create effect

TRADOC Pamphlet 525-3-1

The U.S. Army in Multi-Domain Operations 2028

6 December 2018

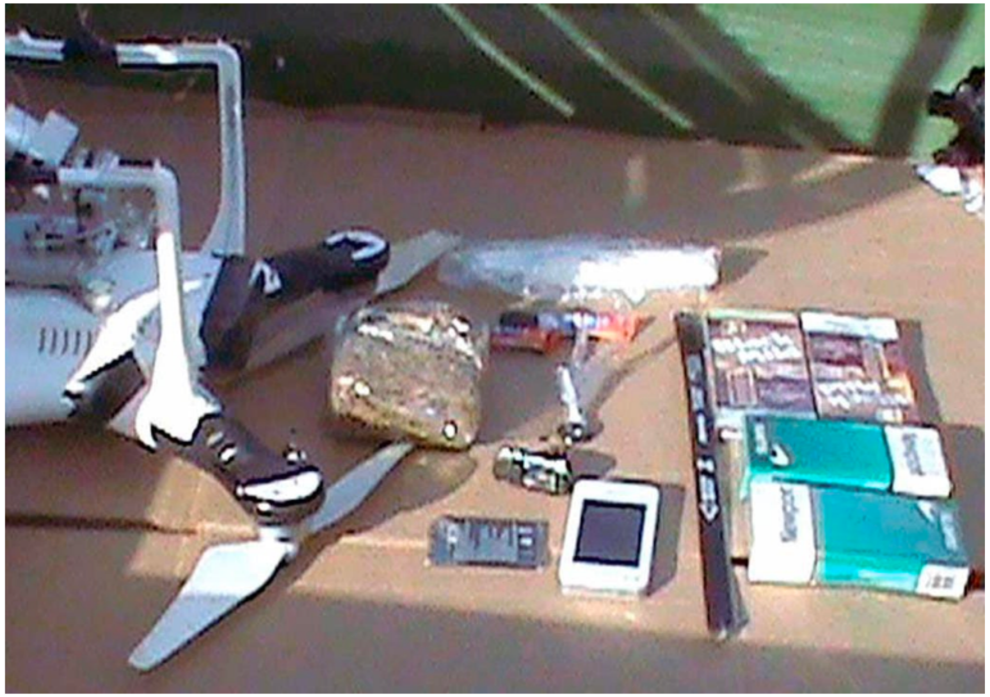
Distribution Statement A.
This document is approved for public release; distribution unlimited.

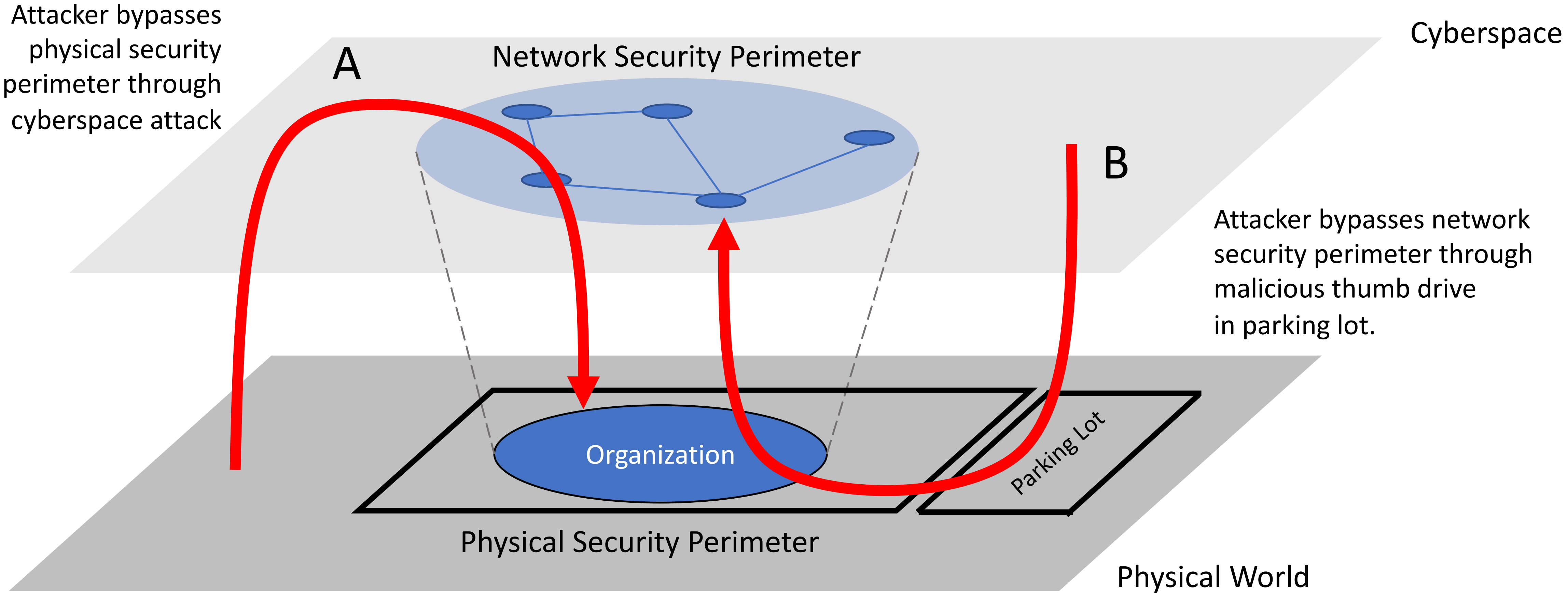
https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf

What Happens When You Fail to Consider a Dimension?

+

=





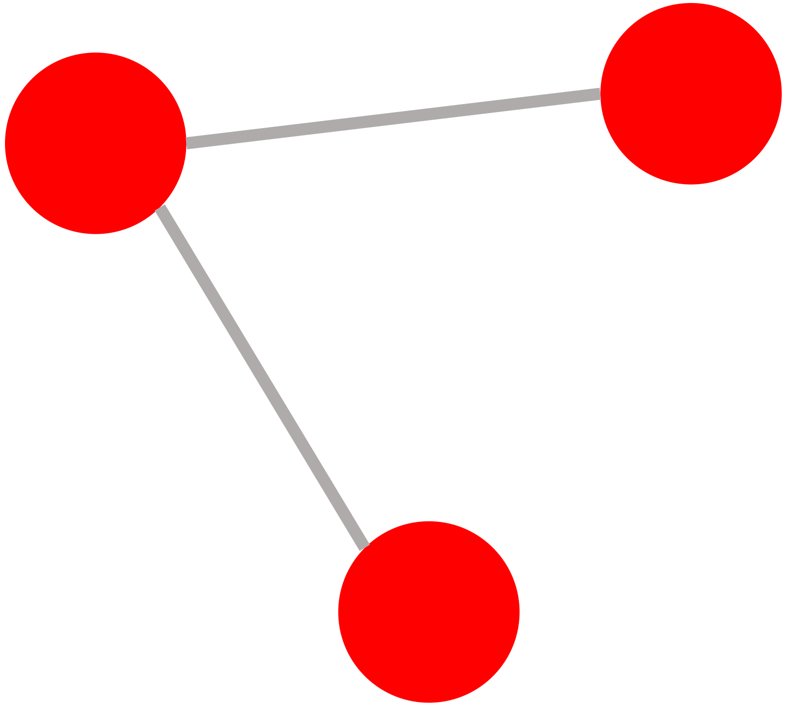
Attacker bypasses physical security perimeter through cyberspace attack

Attacker bypasses network security perimeter through malicious thumb drive in parking lot.

What is Your Organization’s Footprint?

https://file.org.br/artist/joon-y-moon/

Nodes



Node: Nodes are informational or physical entities.

- Nodes store and process information and interact with other nodes via links.
- Examples include: humans, computing systems, social media personas, social media personas
- Can generate effects on other nodes and links.
- For convenience we can aggregate as necessary, and exist on multiple planes.

Call of Duty

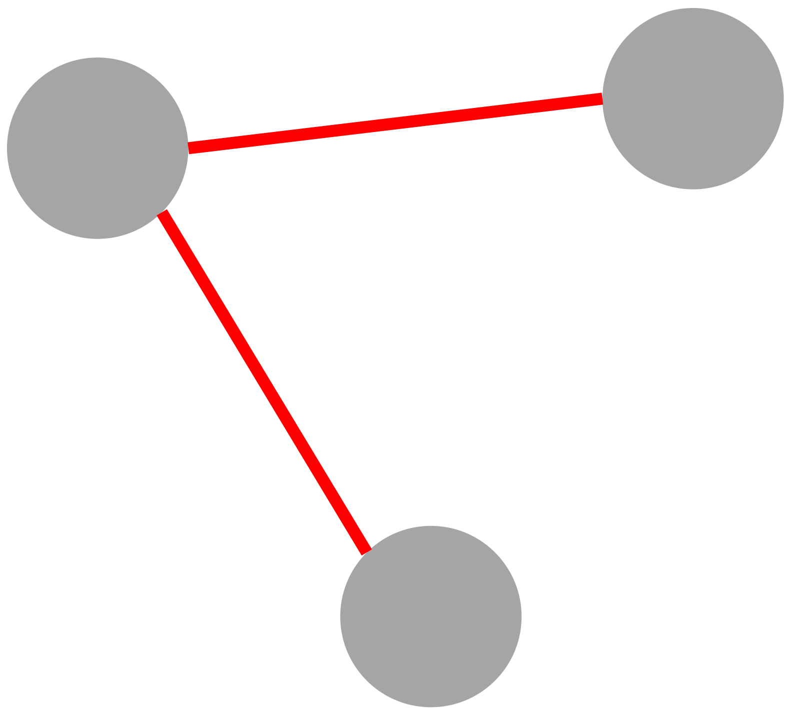
HR System

Government Database

Credit Card Processing

https://aws.amazon.com/blogs/publicsector/tag/data-center/

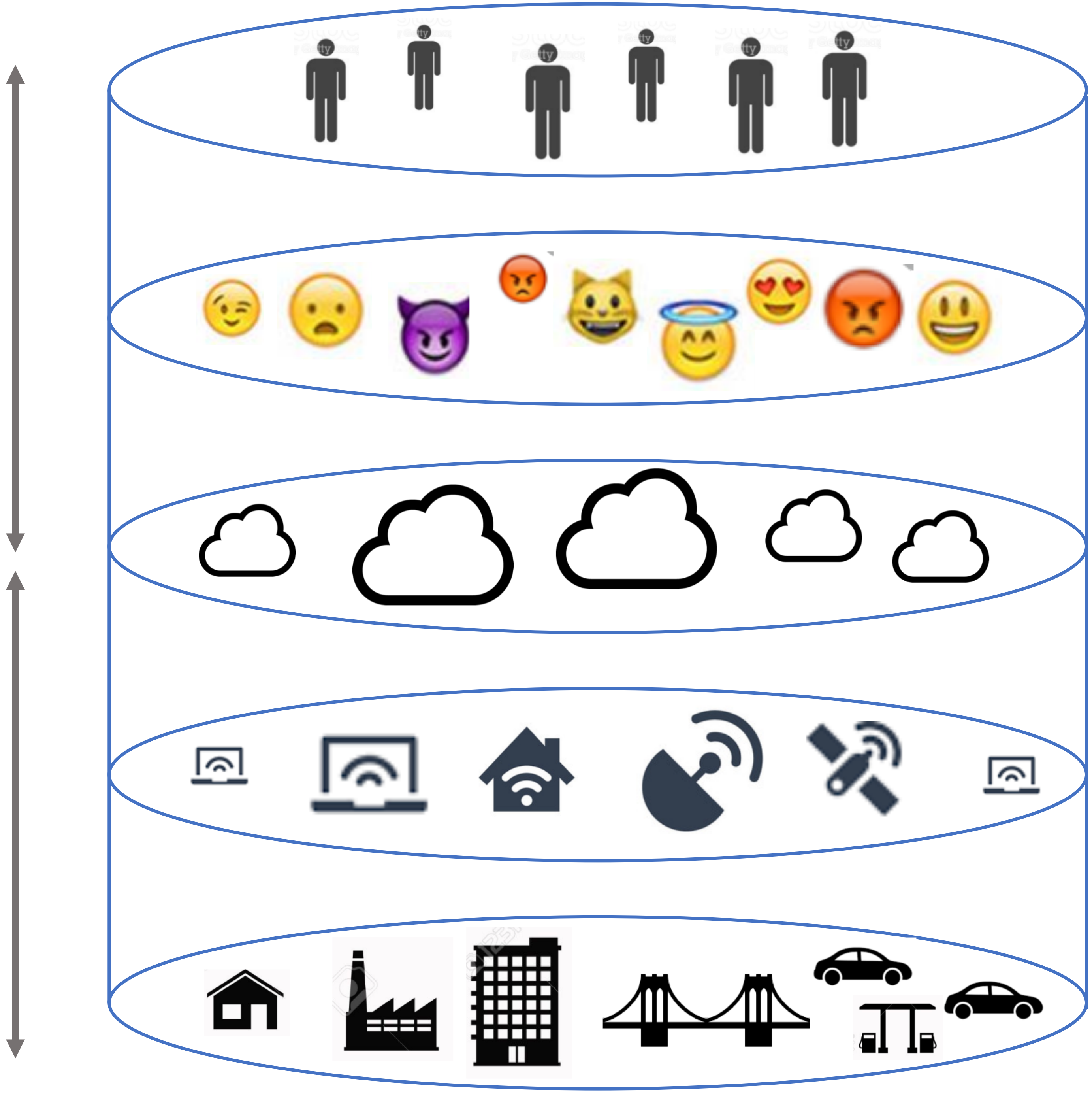
Links



Link: Line of communication or influence between two nodes.

- Links may connect nodes on the same plane or between planes.
  - Same plane: TCP/IP networking, human-to-human interaction
  - Different plane: human-to-machine interface, IT/OT
- Links often comply to protocols (LTE, 802.11, Ethernet, APIs…), except when they don’t.
- Can be bidirectional or unidirectional
- Links enable propagation of desired and undesired effects

ACME
CORPORATION



Human-Computer Interface

IT/OT Interface

Humans

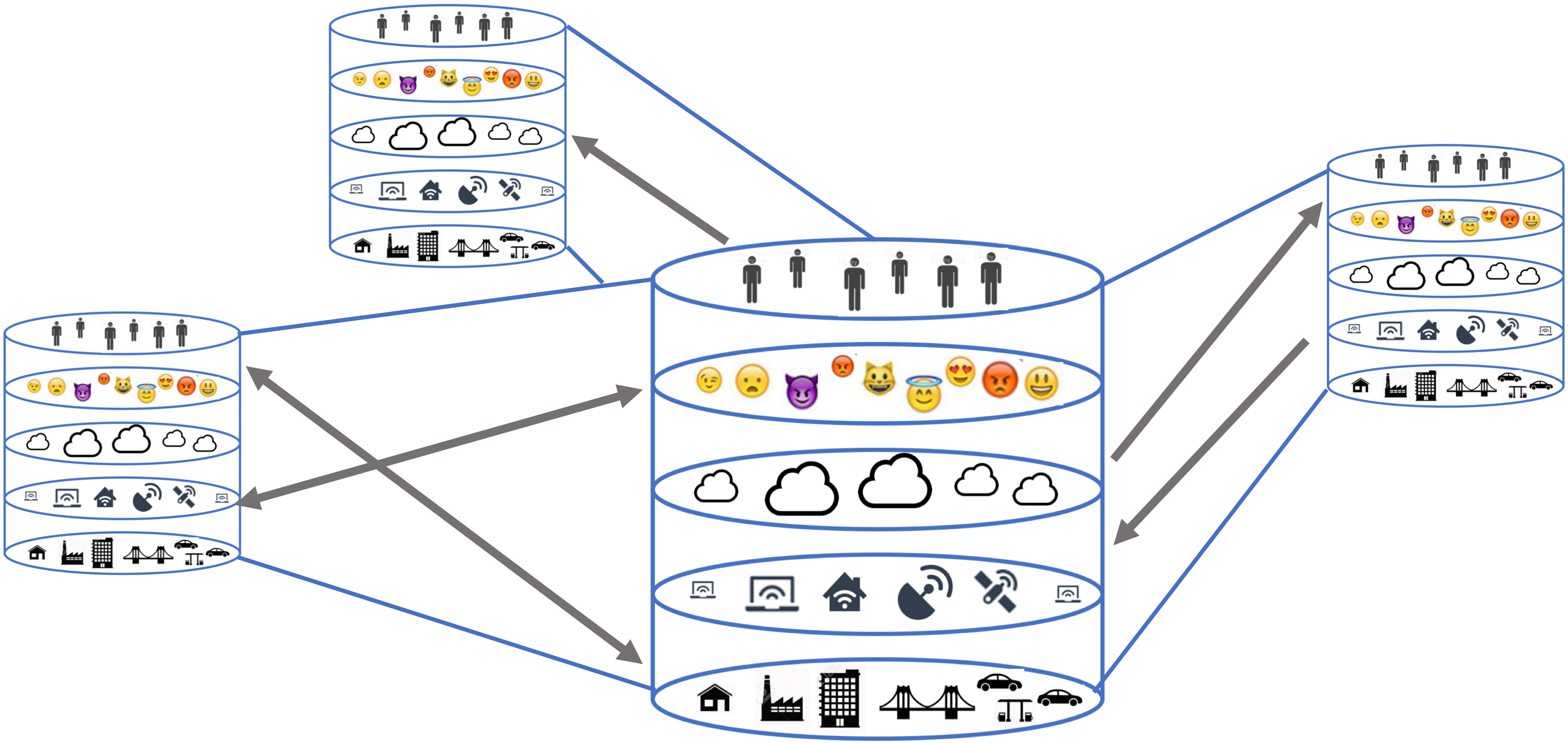
Persona

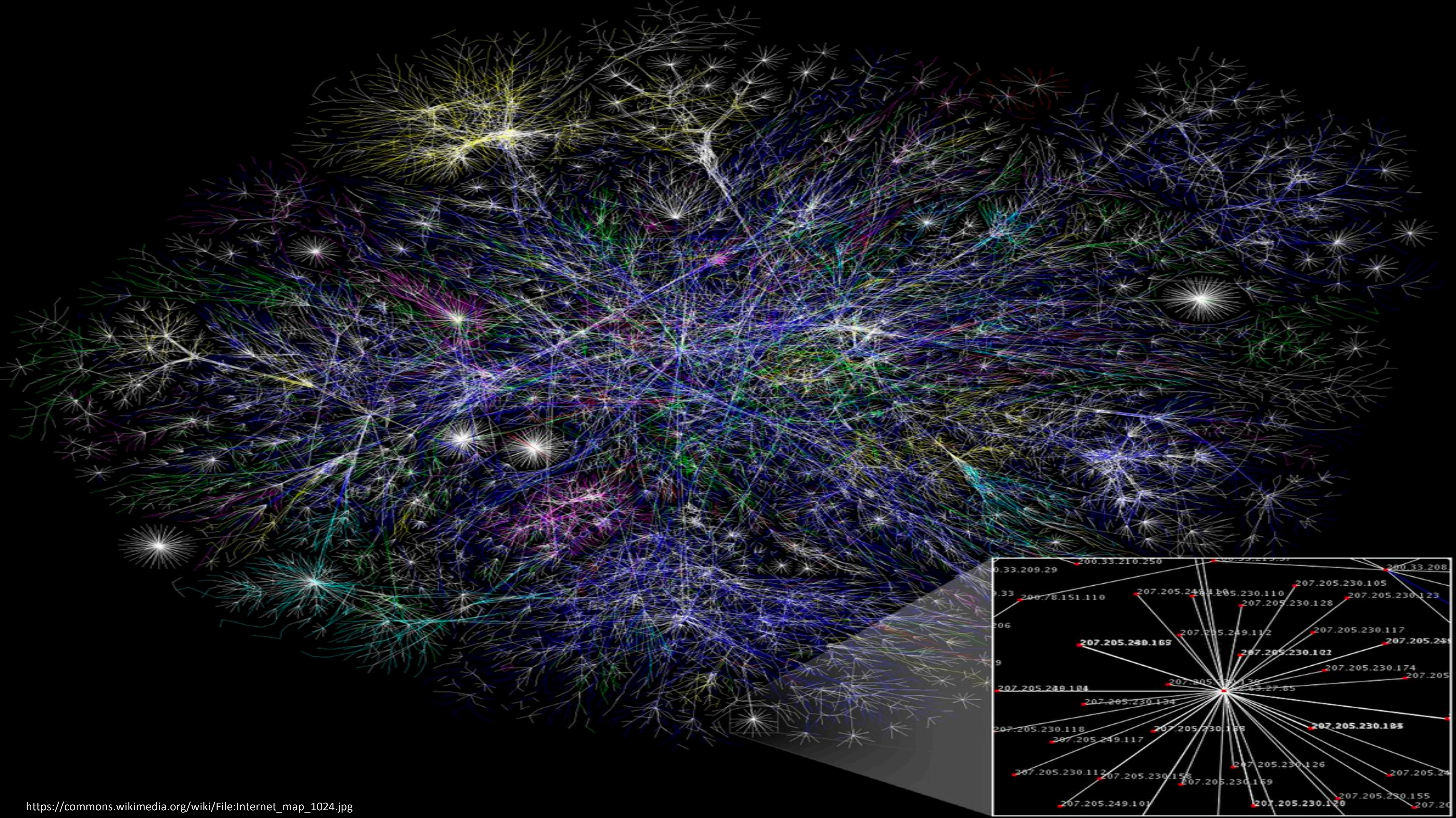
Virtual

Physical

Geographic

ACME
CORPORATION
GLOBEX

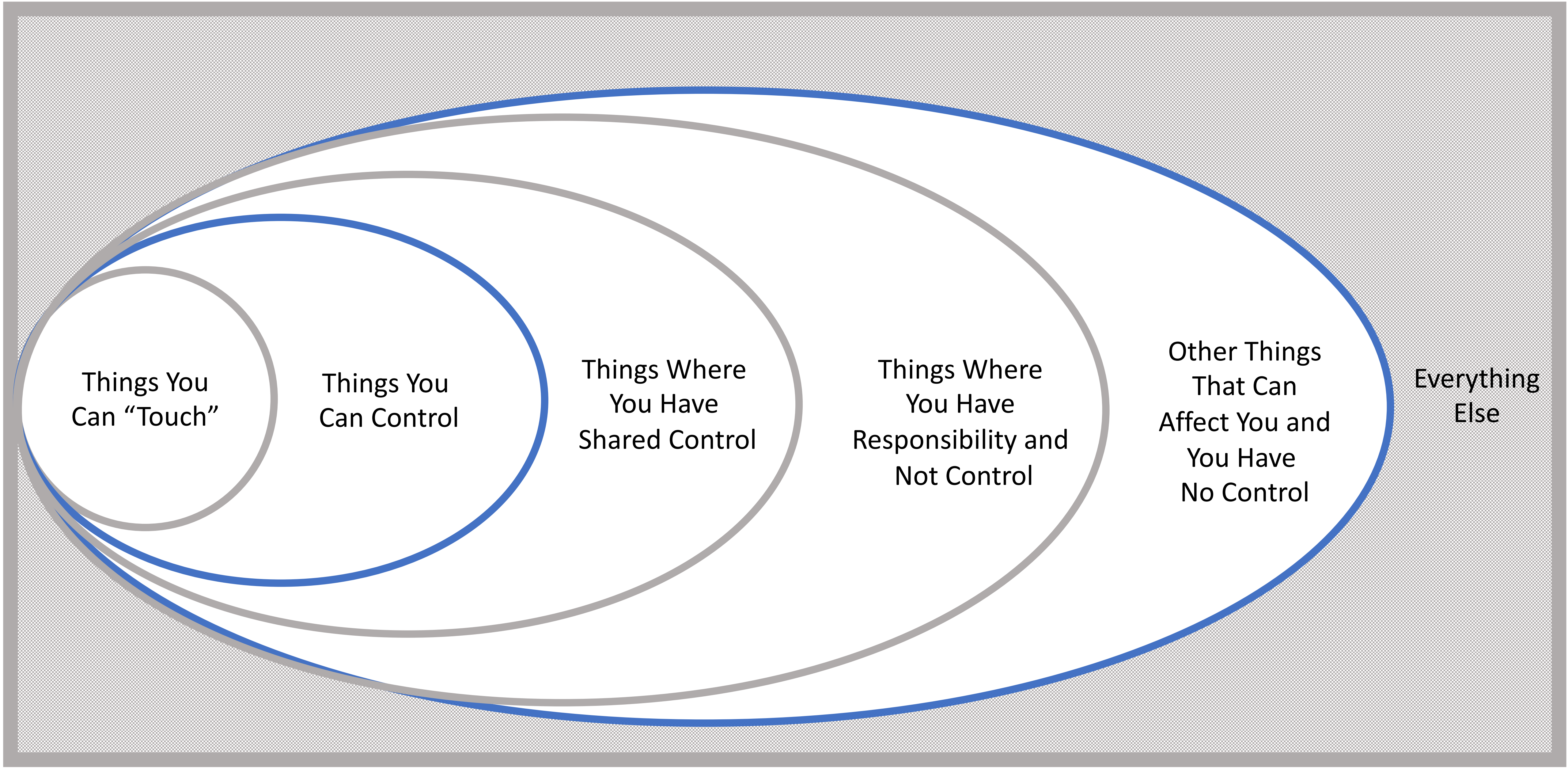




https://commons.wikimedia.org/wiki/File:Internet_map_1024.jpg

Scoping and Coping with Complexity

Degree of Control We Have Over Links and Nodes



Things You Can "Touch"

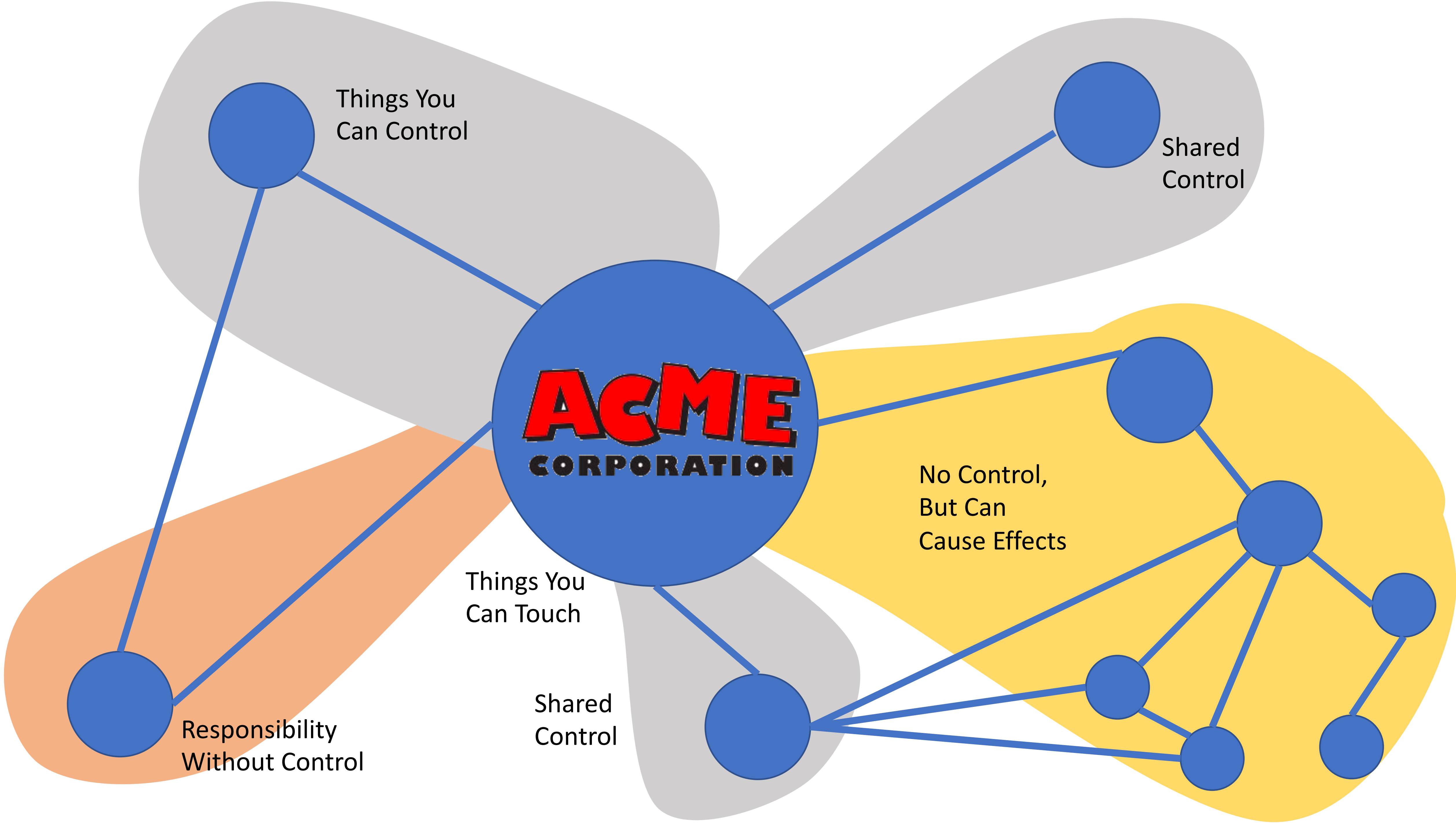
Things You Can Control

Things Where You Have Shared Control

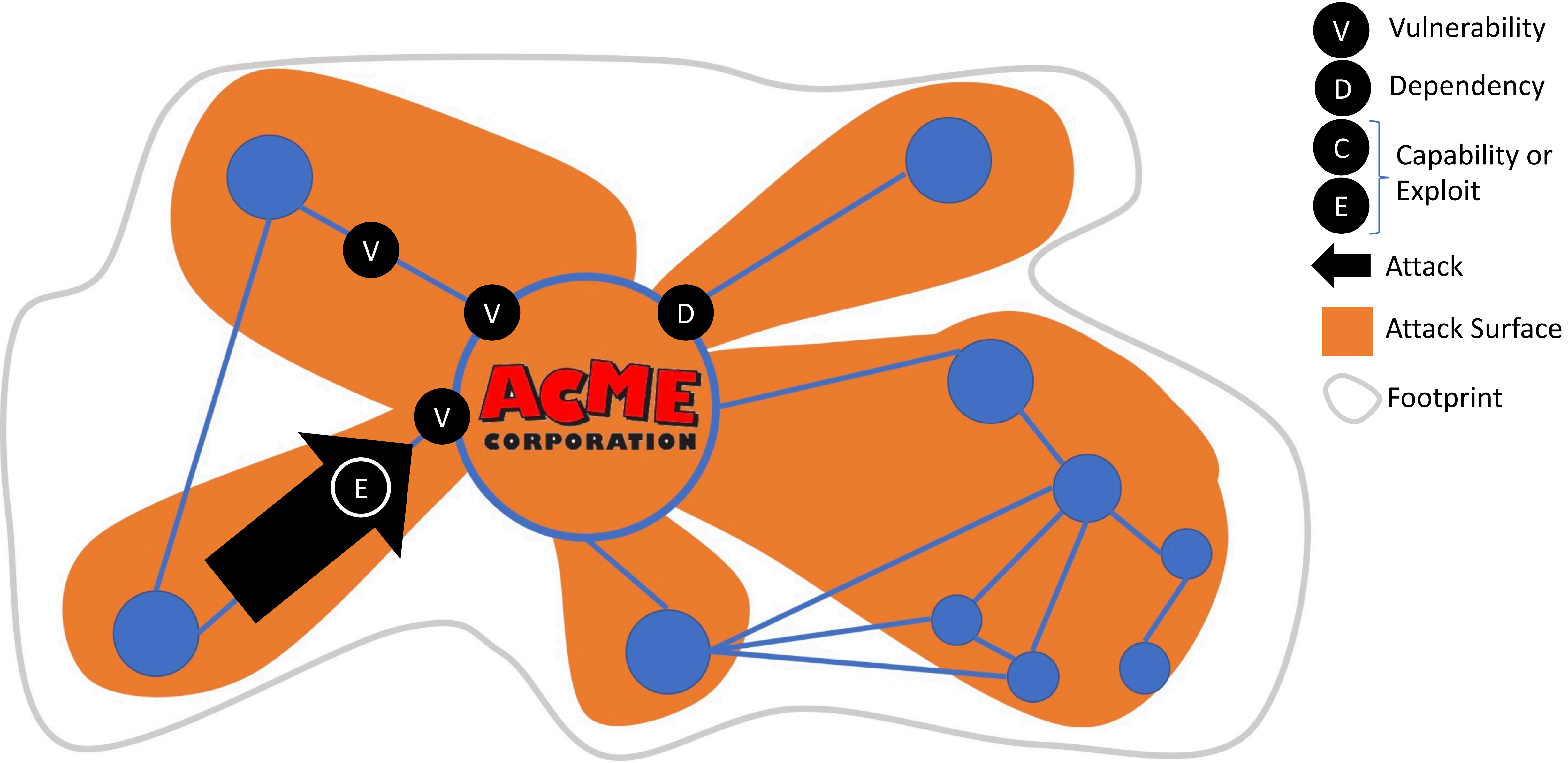
Things Where You Have Responsibility and Not Control

Other Things That Can Affect You and You Have No Control

Everything Else



Things You
Can Control
Shared
Control
ACME
CORPORATION
No Control,
But Can
Cause Effects
Things You
Can Touch
Shared
Control
Responsibility
Without Control



V Vulnerability

D Dependency

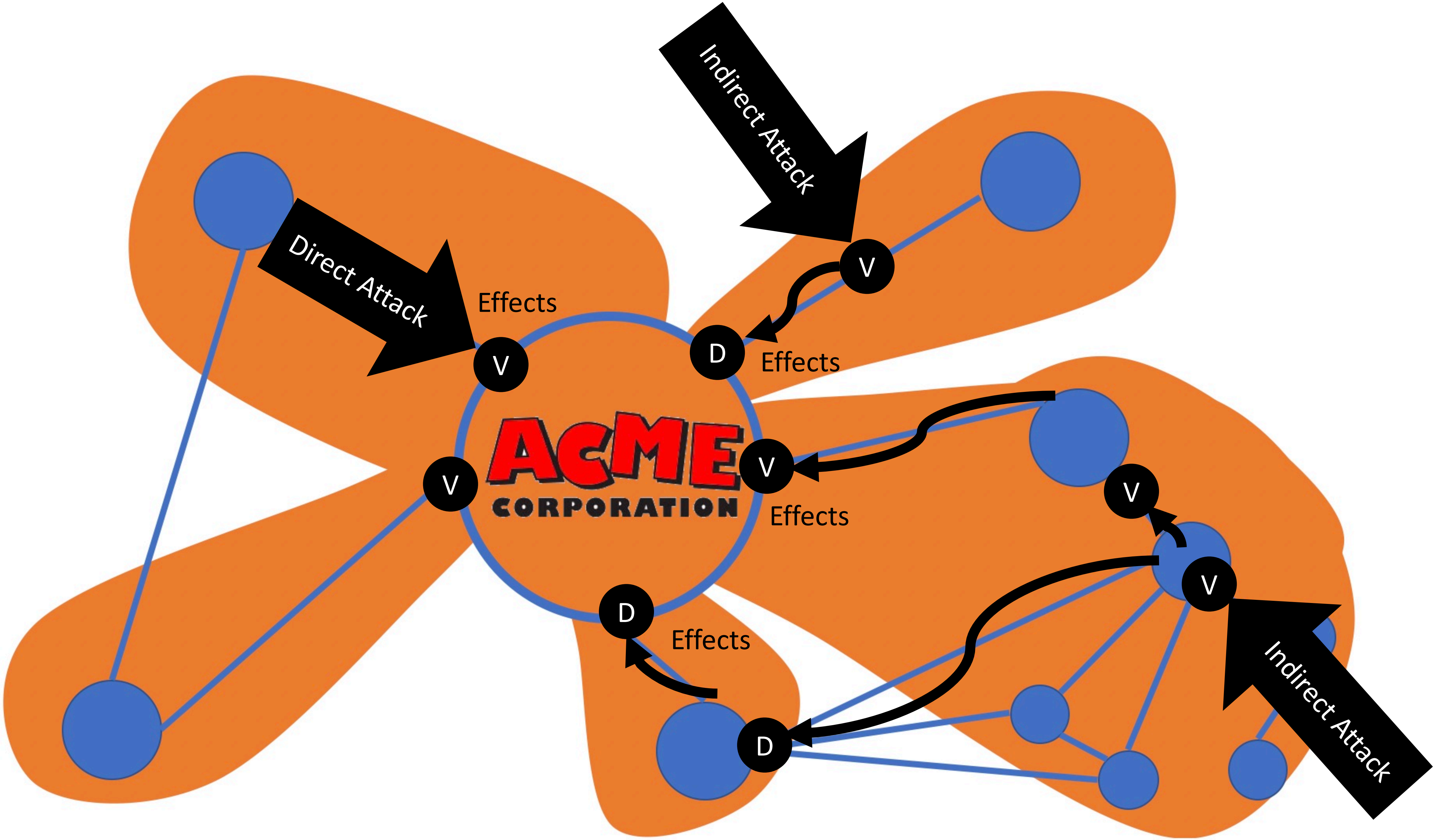
C

E Capability or Exploit

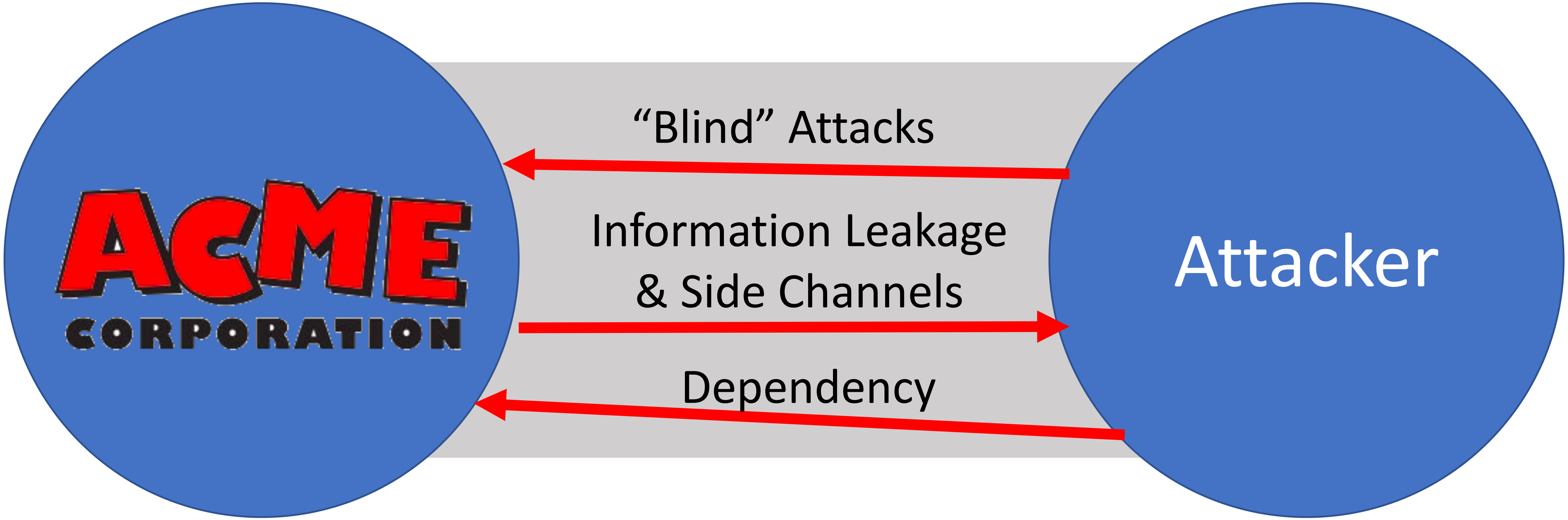
Attack

▨ Attack Surface

○ Footprint


Indirect Attack
Direct Attack
Effects
V
D
Effects
ACME
CORPORATION
V
V
Effects
V
V
D
Effects
D
Indirect Attack

Special Cases



Virtual and Physical Changes over time

Δ

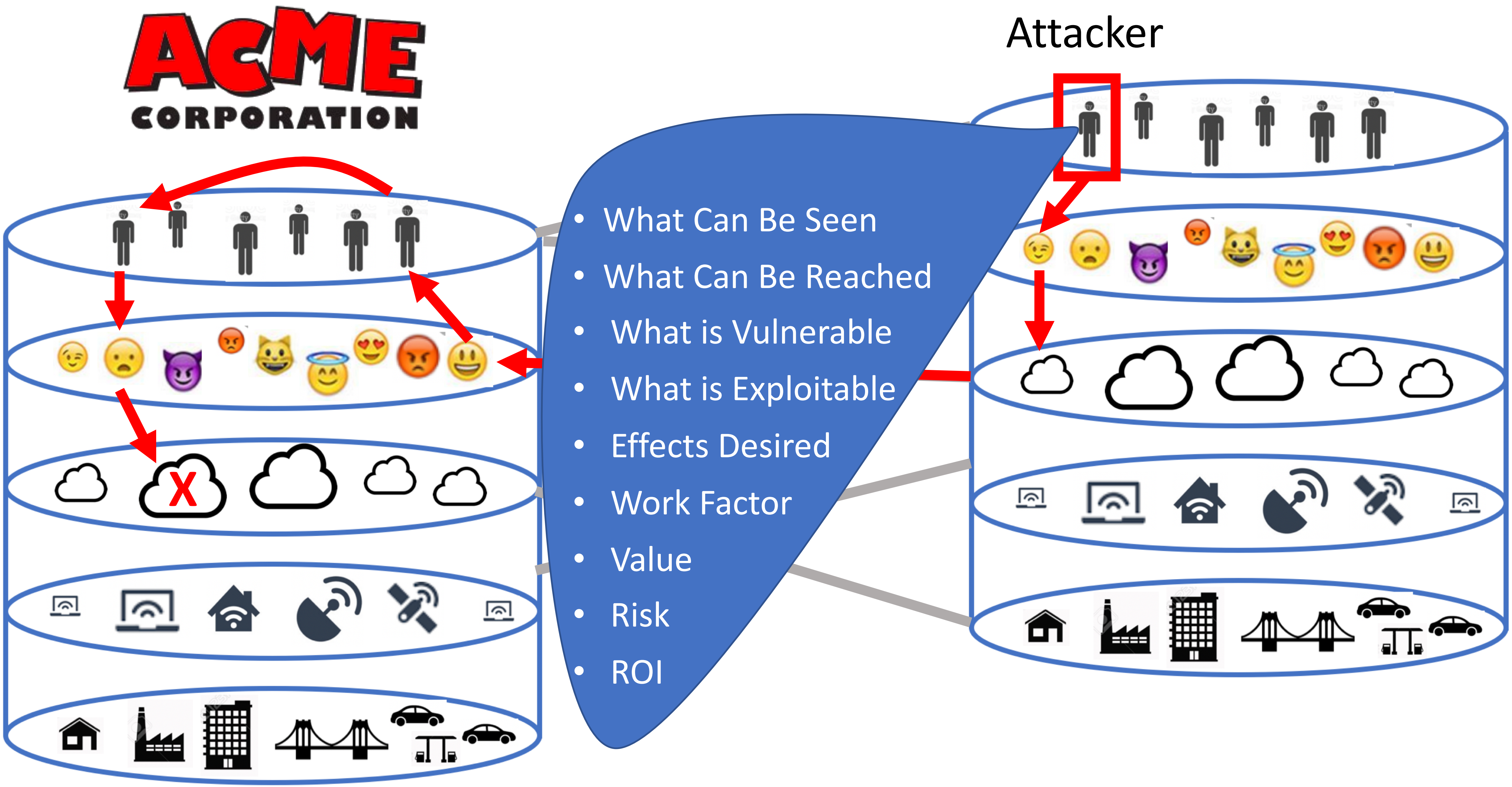
Big Changes

- Mergers and Acquisitions
- Organization shifts to work from home due to COVID
- Moving from data center to a cloud architecture
- OS upgrade to an end point fleet
- Sub-contracting a major project
- Continuous movement of workforce’s cell phones and laptops

δ

Small Changes

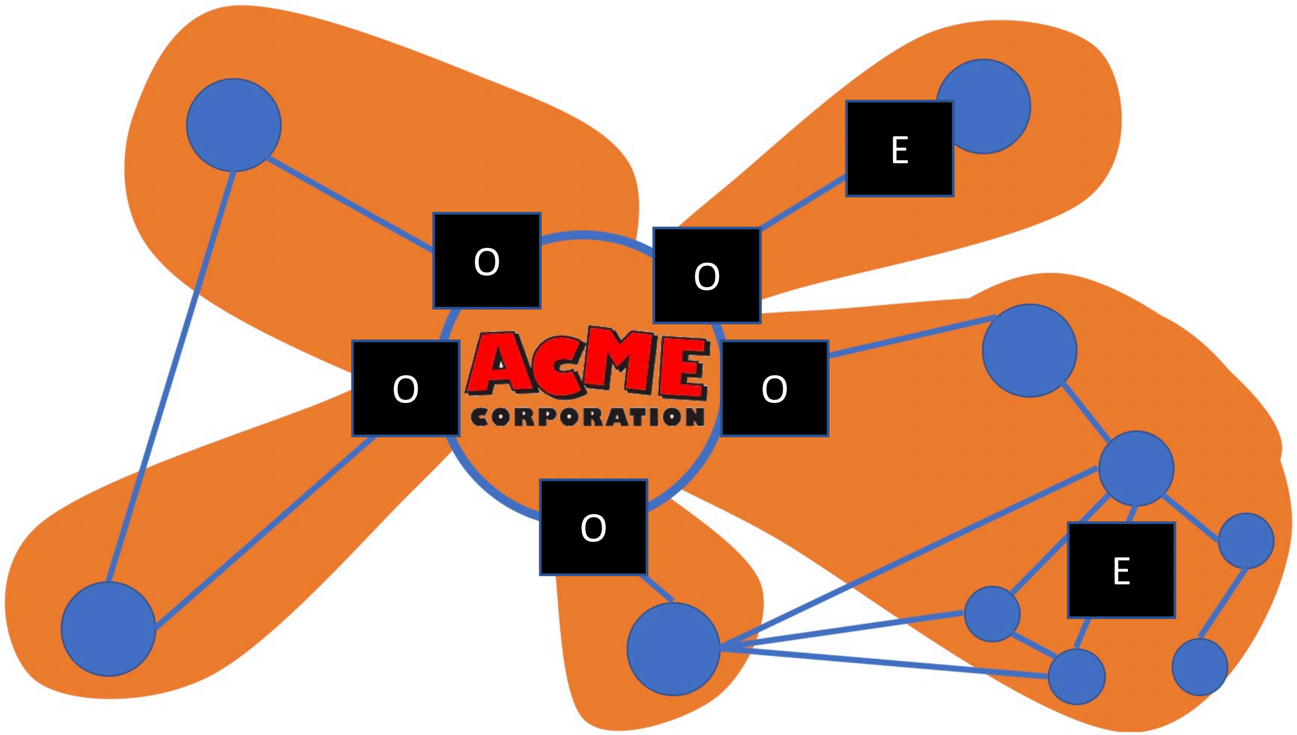
- Patching an endpoint
- Employee comes home and continues work in home office
- Configuring firewall for new 3rd party service
- Employee goes to a conference
- Cosmic rays flip a bit



- What Can Be Seen
- What Can Be Reached
- What is Vulnerable
- What is Exploitable
- Effects Desired
- Work Factor
- Value
- Risk
- ROI

	“Touch”	Control	Shared Control	Responsibility, Not Control	Other Things That Can Affect You
Human	Onsite Workforce	Distributed workforce	Contractors	3rd Party vendors	Family members
Persona	Organizational user accounts	Cloud service accounts	Company social media presence	Company officer social media presence	Influencers, Fraudulent personas
Virtual	On-premises OS and software images	Enterprise cryptographic keys	Cloud services, VPC	3rd Party software updates, Registrar and DNS records, Offsite storage	OS and cloud vulnerabilities, Cryptographic flaws
Physical (Infrastructure)	Data center, On-premises hardware	Remote employee devices, Leased data center	Shared data center/CoLo, Facility OT	BYOD, Rogue hardware, Cloud provider hardware	Network service providers, Undersea cables
Physical (Environmental)	Onsite wireless, Facility HVAC	EM emissions, TEMPEST controls	Licensed EM spectrum, Fire prevention	EM leakage, Audio emanations, Seasonal climate	EM interference, Power failure, Natural disaster
Geographic	Physical locks and keys	Office building security	Shared office building security	Parking lot	Vehicular traffic

Visibility Analysis and Coordinated Cyber Threat Intelligence

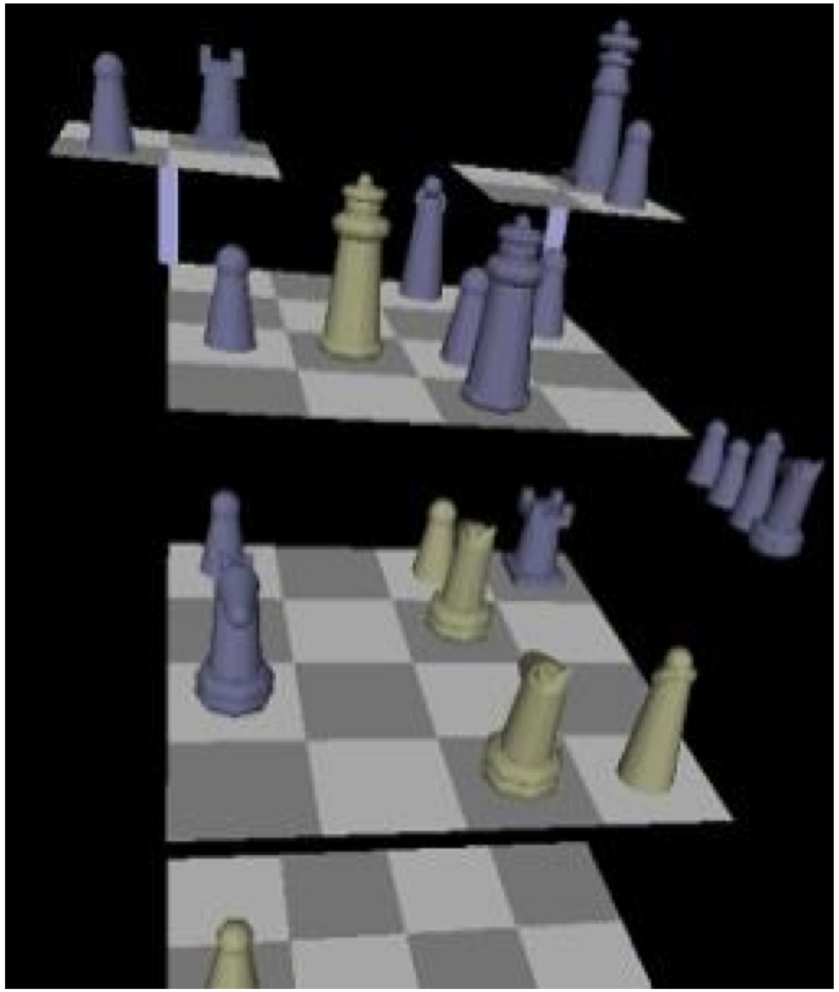


O Organic/Internal Monitoring

E External/Shared Monitoring

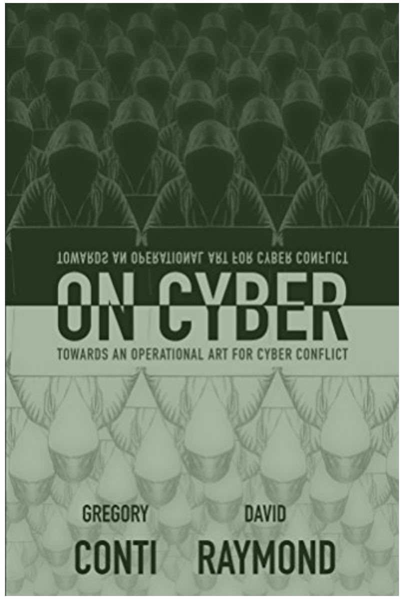
- Place organic (OS) sensor/controls on potential attack vectors across planes
- Use collective defense strategies to place or gain access to external sensors (ES) in blind spots
- Consider inter-organizational threat intelligence collection and sharing
- Prioritize resources to prioritize most dangerous and most likely attack vectors.

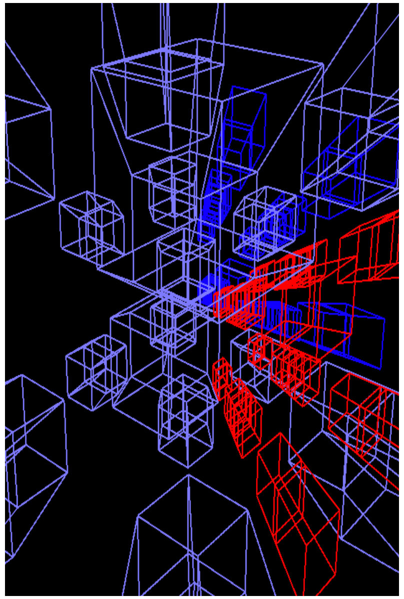
Conclusions and Key Takeaways



- Work to understand the complete footprint of your organization
- Extend your enterprise attack surface analysis…
  - Vertically (across the layers)
  - Horizontally (beyond the enterprise perimeter)
- Use results to…
  - Inform organizational risk management
  - Focus threat intelligence collection
  - Architect more defensible systems
  - Improve placement of security controls
- The methodology is also useful for cities, critical infrastructure sectors, nations, and corporate ecosystems

Where to Go for...





More Information

- Greg Conti and Bob Fanelli, Operational Templates for State-Level Attack and Collective Defense of Countries, Black Hat USA, 2019.
- Greg Conti and Bob Fanelli, Dim Mak: A Study of the Pressure Points that Could Take Down Cyberspace, BSides Long Island, 2019.
- Greg Conti and David Raymond, *On Cyber: Towards and Operational Art for Cyberspace Operations,”* 2016.
- Black Hat Training: Military Strategy and Tactics for Cybersecurity and Information Operations courses
- RiskIQ

Future Work

- Consider things like attack graphs and complex systems analysis.
- N dimensional spaces and vectors, graph theory
- Automated attack surface generation (from attacker and defender perspectives)
- Linking attack surface models with defensive and offensive models
- Software Defined Perimeters

Questions???

Greg Conti
Principal, Kopidion
@cyberbgone

Bob Fanelli
Principal, Kopidion

KOPIDION™

Kopidion.com